R E P U B L I Q U E F R A N

PCT/FR03/03208

#2

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

MAILED 06 JAN 2004
WIPO PCT

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 11 SEP. 2003

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1.a) OU b)

Pour le Directeur général de l'Institut national de la propriété industrielle
Le Chef du Département des brevets

M Heuc

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*03

REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 @ W / 210502

Réservé à l'INPI

REMISE DES PIÈCES DATE 30 OCT 2002
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0213605
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 30 OCT. 2002

Vos références pour ce dossier *(facultatif)* INRIA AFF.58

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET NETTER
36 avenue Hoche
75008 PARIS

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE — Cochez l'une des 4 cases suivantes

Demande de brevet	☒	
Demande de certificat d'utilité	☐	
Demande divisionnaire	☐	
Demande de brevet initiale	N°	Date
ou demande de certificat d'utilité initiale	N°	Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N°	Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Dispositif pour le marquage et la restitution de signaux multimédia

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation — Date — N°
Pays ou organisation — Date — N°
Pays ou organisation — Date — N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases) ☒ Personne morale ☐ Personne physique

Nom ou dénomination sociale		INRIA INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE
Prénoms		
Forme juridique		Etablissement public national à caractère scientifique et technologique
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	Domaine de Voluceau BP 105
	Code postal et ville	7 8 1 5 3 ROCQUENCOURT
	Pays	France
Nationalité		Française
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES DATE 30 OCT 2002
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0213605

DB 540 W / 210502

6 MANDATAIRE *(s'il y a lieu)*		
Nom		PLAÇAIS
Prénom		Jean-Yves
Cabinet ou Société		Cabinet NETTER
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	36 avenue Hoche
	Code postal et ville	7 5 0 0 8 PARIS
	Pays	France
N° de téléphone *(facultatif)*		01 58 36 44 22
N° de télécopie *(facultatif)*		01 42 25 00 45
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		☐ Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint		☐
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		☐
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

Jean-Yves PLAÇAIS N°Conseil 92-1197 (B) (M)

VISA DE LA PRÉFECTURE OU DE L'INPI

M. ROCHET

Dispositif pour le marquage et la restitution de signaux multimédia.

La présente invention concerne un dispositif pour le marquage et la restitution de signaux multimédia.

Le marquage d'un signal multimédia, encore connu sous le nom de procédé de tatouage, consiste à insérer de façon invisible un message dans le signal multimédia avant sa transmission afin de pouvoir le restituer de façon lisible en réception. Pour garantir le secret du message inséré, un ensemble de clés privées ou publiques est souvent utilisé afin de ne pas offrir la possibilité à des personnes non autorisées de retrouver, voir d'enlever le message caché.

Les domaines d'application d'un procédé de marquage de signaux multimédia sont nombreux.

Tout d'abord, dans un contexte de protection, il peut être intéressant d'insérer dans le contenu d'un signal multimédia un message caché permettant par la suite d'identifier ce contenu, de connaître le propriétaire de ce contenu ou bien encore de connaître les règles d'utilisation de ce contenu, telles que par exemple le droit de diffusion ou le droit de copie.

Cependant, le contenu du message multimédia peut être altéré de différentes façons. Par exemple, il peut être altéré suite à l'utilisation d'un format de représentation introduisant des dégradations, tel qu'un codage avec perte (par exemple, JPEG pour les images fixes, MPEG pour la vidéo ou bien encore MP3 pour l'audio) ou bien encore par divers procédés d'acquisition tels que l'enregistrement analogique, l'impression ou le "scanning" pour une image.

Le contenu d'un signal multimédia peut aussi être altéré suite à une remise en forme, par exemple lors d'une sélection d'une portion d'un fichier audio ou lors du recadrage d'une image.

Le contenu d'un signal multimédia peut aussi subir des attaques intentionnelles dans le but de mettre à défaut le procédé d'extraction du message. Ceci peut être effectué en ajoutant du bruit au signal, en utilisant une technique de filtrage ou en utilisant des techniques désynchronisantes (par exemple, la transformation géométrique pour les images ou le changement de fréquence pour les fichiers sonores). Dans ce cadre d'applications, il est important d'assurer que le message inséré puisse être extrait correctement que le contenu ait subi des modifications intentionnelles ou non.

Un autre cadre d'applications concerne la mise à disposition, grâce à un procédé de tatouage, d'un canal de transmission d'informations de façon non perceptible et lié au contenu lui-même des signaux multimédia. En particulier, ceci peut être intéressant dans le cas d'un transcodage ou d'une diffusion ultérieure du contenu, où l'existence et/ou la pérennité d'un tel canal de transmission n'est pas garantie. Ce canal adjacent peut alors être utilisé, suivant sa capacité, pour transmettre toute information utile. On peut citer à titre d'exemple l'insertion de méta-données décrivant le contenu tatoué (telles que l'identifiant du contenu ou la description d'éléments du contenu) qui peuvent être utilisées ultérieurement afin d'assurer un service à valeur ajoutée, ou bien encore des informations annexes (telles qu'un service de type télétexte ou des sous-titres). Ici encore, il est important de pouvoir extraire ces informations suite à différentes manipulations du contenu, principalement du transcodage et donc de disposer d'un système de tatouage robuste.

Dans des dispositifs de marquage connus, on utilise une technique de modulation de type COFDM, couramment utilisée en communication numérique, où des bits bj définissent le message et sont modulés par plusieurs porteuses définies par des clés publiques et privées. Le signal ainsi modulé vient s'ajouter au signal original. A l'extraction, une démodulation permet de retrouver les bits insérés bj. Cependant cette technique de marquage souffre d'imperfections car le signal hôte peut interférer sur les porteuses utilisées, le signal inséré peut être visible ou encore la re-synchronisation peut être imparfaite.

Le but de l'invention est de remédier à cette situation.

L'invention propose à cet effet un dispositif de traitement d'un signal comprenant un module de transformation de signal capable de produire un signal transformé à partir d'un signal

original et un module mélangeur destiné à marquer le signal transformé par un message de marquage. Selon une caractéristique de l'invention, le module mélangeur comprend :

- un module de mise en forme capable de calculer une réponse du signal transformé à la démodulation d'un premier ensemble de porteuses définies par des clés de protection du message et de calculer une information de marquage en fonction de cette réponse et de mots de codes associés au message de marquage,
- un modulateur capable de moduler les informations de marquage fournies par le module de mise en forme par un coefficient donné des porteuses du premier ensemble de porteuses, et de moduler en amplitude le coefficient ainsi obtenu par une quantité correspondante liée au terme de pondération de l'énergie du message de marquage et à l'ensemble de porteuses, ce qui fournit un coefficient de marquage,
- un additionneur capable d'ajouter le coefficient de marquage au coefficient correspondant du signal original transformé.

La modulation d'amplitude effectuée par le modulateur permet ainsi de rendre le signal ajouté peu visible. De plus, le dispositif de l'invention met en oeuvre une technique de codage canal avec information de bord. Selon cette technique, les composantes de l'information de marquage sont des informations à valeurs flottantes définies de telle façon que leur insertion compense la réponse du signal hôte.

Selon une autre caractéristique de l'invention, le module de mise en forme comprend un démodulateur destiné à effectuer la démodulation, ce démodulateur étant apte à multiplier chaque coefficient du signal transformé par le coefficient correspondant d'une porteuse donnée du premier ensemble de porteuses, par le poids perceptuel de distorsion et par le facteur d'atténuation associés au coefficient du signal transformé, et à additionner les coefficients ainsi déterminés, ce qui fournit une composante de la réponse du signal transformé.

Le module de mise en forme est également apte à calculer l'information de marquage à partir d'un paramètre prédéterminé, d'un premier vecteur associé à un mot de code particulier du message de marquage et d'un deuxième vecteur formant avec ledit premier vecteur une base orthogonale normalisée définissant un hyperplan.

En particulier, le mot de code particulier est obtenu en minimisant un critère d'erreur quadratique entre les mots de code associés au message de marquage et la valeur normalisée de la réponse du signal transformé à la démodulation.

Chaque composante du deuxième vecteur est proportionnelle à la différence entre la composante correspondante de la réponse à la démodulation et la projection du vecteur représentant la réponse à la démodulation sur un vecteur unitaire colinéaire au premier vecteur.

Le paramètre prédéterminé correspond à l'angle entre le vecteur représentant l'information de marquage et le premier vecteur, ce paramètre étant déterminé en maximisant la relation:

$$K.(uo + \cos\theta)^2 - (vo + \sin\theta)^2$$

dans laquelle:

- uo représente le produit scalaire entre le vecteur représentant la réponse à la démodulation et le premier vecteur, divisé par le nombre m de composantes de la réponse à la démodulation,
- vo représente le produit scalaire entre le vecteur représentant la réponse à la démodulation et le deuxième vecteur, divisé par le nombre m,
- $K = 1/(2^{2.(C+R)/m} - 1)$, C et R représentant respectivement le nombre de bits utiles et de bits d'adaptation au signal original et m représente le nombre de composantes de la réponse à la démodulation.

Selon une autre caractéristique de l'invention, le mélangeur comporte un module de mise à l'échelle capable de moduler en amplitude chaque coefficient du signal fourni par le circuit additionneur par une quantité liée au terme de pondération de l'énergie du message de marquage et de la variance du coefficient correspondant du signal transformé.

Cette quantité est définie par $\sigma_{xi}^2 / (\sigma_{xi}^2 + \sigma_{wi}^2)$, où σ_{xi}^2 est le terme définissant l'énergie du message de marquage et σ_{xi}^2 est la variance du coefficient correspondant du signal transformé.

Cette modulation d'amplitude correspond à un filtre de Wiener et permet de limiter le bruit ainsi ajouté sur le signal hôte.

Selon une autre caractéristique de l'invention, le dispositif comporte un module de transformation inverse en sortie du mélangeur, apte à effectuer sur le signal marqué une transformation inverse de celle effectuée par le module de transformation, et un module de transformation de signal apte à transformé le signal marqué resynchronisé, ce qui fournit un signal marqué transformé.

Le dispositif peut également comporter un dispositif d'extraction en sortie du module de transformation inverse pour extraire le message du signal marqué, ce dispositif d'extraction comportant un module de resynchronisation capable de resynchroniser le signal marqué.

En particulier, le dispositif d'extraction est capable de calculer une réponse du signal marqué resynchronisé à la démodulation d'un deuxième ensemble de porteuses définies par des clés de protection du message, ce qui fournit une estimation de l'information de marquage insérée.

Dans une variante de réalisation, le premier ensemble de porteuses et le deuxième ensemble de porteuses sont identiques.

Par ailleurs, le dispositif d'extraction peut comprendre un démodulateur destiné à effectuer la démodulation, ce démodulateur étant apte à multiplier chaque coefficient du signal marqué resynchronisé par le coefficient correspondant d'une porteuse donnée du deuxième ensemble de porteuses et par le poids perceptuel de distorsion associé audit coefficient du signal marqué resynchronisé, et à additionner les coefficients ainsi déterminés, ce qui fournit une composante de l'estimation de l'information de marquage.

En complément, le dispositif d'extraction peut comporter un module générateur de porteuses propres à générer le deuxième ensemble des porteuses à partir des clés de protection du message.

Le dispositif d'extraction peut aussi comporter un décodeur capable de déterminer le mot de code le plus proche de l'estimation de l'information de marquage en maximisant un critère d'erreur quadratique entre un ensemble de mots de code et l'estimation de l'information de marquage, ce qui fournit le message de marquage.

Selon une autre caractéristique de l'invention, le dispositif de traitement peut également comprendre un module de définition de paramètres d'insertion couplé au module mélangeur capable de déterminer le terme de pondération de l'énergie du message de marquage et le facteur d'atténuation à partir des propriétés intrinsèques du signal, des contraintes du domaine applicatif, et des propriétés de la transformation utilisée.

En particulier, le module de définition de paramètres d'insertion est capable de calculer deux paramètres globaux d'insertion en fonction de la distorsion d'insertion D_{xy} entre le signal original et le signal marqué dans l'espace transformé, de la distorsion d'attaque maximale tolérée $D_{xy'}$ entre le signal original et le signal marqué resynchronisé, dans l'espace transformé, et du rapport signal à bruit entre l'énergie du message de marquage et le bruit d'attaque Eb/No.

Les deux paramètres globaux d'insertion sont calculés en recherchant les paramètres λ et χ qui maximise la relation:

$Eb/N_0 + \lambda D_{xy'} - \chi D_{xy}$.

Le module de définition de paramètres d'insertion est apte à calculer le terme de pondération de l'énergie du message de marquage et le facteur d'atténuation à partir des deux paramètres globaux d'insertion déterminés.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'aide de la description qui suit et des figures des dessins annexés dans lesquels:

- la figure 1 illustre la composition d'un système de transmission de signaux multimédia marqués pour la mise en oeuvre de l'invention,
- la figure 2 est une organisation générale du dispositif d'insertion de la figure 1,
- la figure 3 est une organisation générale du dispositif d'extraction de la figure 1,
- la figure 4 est un schéma fonctionnel du module d'insertion de la figure 2,
- la figure 5 est un schéma fonctionnel du module mélangeur de la figure 4,
- la figure 6 est une représentation graphique permettant d'apprécier la robustesse d'un signal, suite à l'ajout de bruits d'énergie donnée,
- la figure 7 est un schéma fonctionnel d'un mode de réalisation du module d'extraction de la figure 3, et
- la figure 8 est le schéma d'un mécanisme utilisé dans un mode de réalisation.

L'annexe I répertorie les diverses notations utilisées dans la description.
L'annexe II répertorie les formules mathématiques utilisées dans la description.

Les dessins et les annexes à la description comprennent, pour l'essentiel, des éléments de caractère certain. Ils pourront donc non seulement servir à mieux faire comprendre la description, mais aussi contribuer à la définition de l'invention, le cas échéant.

Le dispositif pour le marquage et la restitution de signaux multimédia pour la mise en oeuvre de l'invention, représenté schématiquement sur la figure 1, se compose d'un dispositif d'insertion d'un message marqueur 1 et d'un dispositif d'extraction du message marqueur 2.

Le dispositif d'insertion de message 1 élabore un marquage d'un signal multimédia S à transmettre au travers d'un domaine applicatif 3, à partir du contenu d'un message marqueur M. La technique de marquage utilisée est une technique additive mettant en oeuvre un procédé de modulation par étalement de spectre. Elle s'apparente à la technique de modulation de type COFDM couramment utilisée en communication numérique. Les composantes bj qui définissent le message marqueur M sont modulées par des porteuses définies par des clés publiques et privées, et appliquées à l'entrée du dispositif d'insertion. Le signal ainsi modulé vient s'ajouter au signal original S. A l'extraction, une démodulation permet de retrouver les composantes insérées bj du message marqueur.

Selon une caractéristique avantageuse de l'invention, pour garantir un bon niveau de robustesse et pour éviter que le signal inséré ne soit visible, une modulation d'amplitude du signal ajouté est effectuée en fonction de l'énergie de la marque ajoutée à chaque coefficient du signal dans le domaine transformé. Suite à cet ajout, une autre modulation d'amplitude est effectuée sur chaque coefficient marqué. Cette deuxième modulation correspond à un filtre de Wiener visant à limiter le bruit ainsi ajouté sur le signal hôte.

Traditionnellement, les composantes bj correspondent aux bits définissant le message à insérer après une éventuelle utilisation de codes correcteurs. Dans le schéma ici présenté, une technique de codage canal avec information de bord est utilisée. Les composantes bj de ce modèle de marquage sont alors des informations à valeurs flottantes.

Le procédé de marquage, décrit ci-après, prend en compte un tel modèle de marquage et l'optimise afin de résister à des attaques du type ajout de bruit, filtrage et désynchronisation partielle, modélisant assez bien les différents traitements que peut subir un signal.

Le dispositif d'insertion, représenté sur la figure 2 comprend un module d'insertion 4 couplé en amont à un module de transformation 5 et en aval à un module de transformation inverse 6. Dans cette configuration, le signal original S, défini dans un premier espace, est appliqué au module de transformation 5 pour être transformé en un nombre n de coefficients xi, définis dans un deuxième espace. Tout procédé de transformation peut être mis en oeuvre sans exclure la transformation identité qui amène à travailler directement sur le signal original. Différentes transformations peuvent être utilisées, comme par exemple la transformation de Fourier, la transformation en cosinus discrets ou la transformation en ondelettes.

Après transformation du signal original S, le message M à insérer est appliqué dans le module d'insertion 4 sur les différents coefficients xi du signal transformé pour former des coefficients marqués yi. Les coefficients marqués yi sont ensuite appliqués au module de transformation inverse 6 afin de subir une transformation inverse de celle appliquée avant marquage et restituer ainsi un signal marqué proche du signal original. Ce signal marqué est alors transmis à un dispositif d'extraction, comme représenté à la figure 3.

Sur la figure 3, le dispositif d'extraction 2, qui est représenté à l'intérieur d'une ligne fermée en pointillés, comprend un module de transformation 7 couplé en amont à un module de resynchronisation 8 et en aval à un module d'extraction 9. Le signal marqué reçu est tout d'abord resynchronisé par le module de resynchronisation 8, puis transformé par le module de transformation 7 en une suite de coefficients yi' par une transformation identique à celle qui a été utilisée lors de l'insertion. Les coefficients yi' sont ensuite appliqués au dispositif d'extraction 9 pour extraire le signal de marquage M. Le procédé de resynchronisation utilisé peut être quelconque (recherche exhaustive liée à l'insertion d'un signal pilote ou à une propriété intrinsèque de la marque) ou bien encore implicite grâce à l'insertion dans un domaine invariant aux désynchronisations (par exemple, amplitudes dans un domaine de Fourier ou transformation de Fourier-Mellin).

Dans la description qui suit, les notations de l'annexe I sont utilisées.

Un mode de réalisation du module d'insertion 4 est représenté sur la figure 4, à l'intérieur d'une ligne fermée en pointillés. Ce module comprend un module mélangeur 10, un module d'analyse du signal 11, un module d'analyse des propriétés intrinsèques 12 et un module de définition de paramètres d'insertion globaux 13.

L'insertion d'un message M dans un signal de coefficients xi débute dans le module 11 par une analyse qui permet de définir les propriétés liées au signal, à savoir le poids de pondération perceptuel dans la métrique de distorsion φi, défini pour chaque coefficient xi du signal original transformé en fonction de la valeur de la variance σ_{xi}^2 du coefficient correspondant. Le poids de pondération perceptuel φi de chaque coefficient xi du signal est fonction du type du signal traité, de la transformation utilisée et des valeurs du signal observé.

Afin d'estimer les variances σ_{xi}^2 du signal (Annexe I-1), tout procédé peut être utilisé. On peut, par exemple, utiliser une moyenne quadratique pondérée dans un voisinage (ou moyenne quadratique glissante), selon la relation (2) de l'annexe II de la description. Dans cette relation, vi représente un voisinage du coefficient considéré.

La valeur naïve $\varphi i = 1$ correspond à l'erreur quadratique moyenne classique. Un exemple de modèle plus adapté pour les images prenant en compte les phénomènes de masquage peut être défini par la relation (3), exprimée dans l'annexe II à la description. Dans cette relation, σ_{bi}^2 correspond à un seuil de visibilité pour le i-ème coefficient, et Vi correspond à un facteur de force de masquage local défini par une moyenne glissante sur le voisinage vi du coefficient considéré, selon la relation (4) de l'annexe II. ρ est un paramètre de l'ordre de 0.5 à 1 (typiquement les valeurs 0.5, 0.6 et 0.7 sont les plus couramment utilisées).

A partir des contraintes applicatives et des propriétés de la transformation utilisée, des paramètres applicatifs ai, bi et ci sont déterminées par le module d'analyse des propriétés intrinsèques 12, pour chaque coefficient xi. Le paramètre ai représente le degré d'interférence avec le signal original, le paramètre bi le degré d'auto interférence du signal inséré et le paramètre ci est le paramètre d'atténuation du site.

Les paramètres applicatifs ai, bi et ci permettent de prendre en compte un phénomène de désynchronisation sur chaque site, c'est à dire sur chaque fréquence porteuse de l'espace

transformé. Par exemple, pour une désynchronisation Δ_i sur le i-ème site, représentant la précision de la localisation du coefficient, on utilisera typiquement les valeurs définies par les relations (5) de l'annexe II à la description.

A partir des paramètres φi, σ_{xi}^2, ai, bi et ci fournis par les modules 11 et 12, le module 13 estime les paramètres globaux d'insertion λ et χ. A partir de ces paramètres globaux d'insertion, le module 13 détermine ensuite les paramètres d'insertion γi et σ_{wi}, définissant les propriétés intrinsèques du signal de marquage. Le premier paramètre d'insertion γi représente le facteur d'atténuation du site considéré et le deuxième paramètre d'insertion σ_{wi} représente le terme de pondération de l'énergie de marquage.

Une fois les différents paramètres établis, l'insertion du message M dans le signal transformé {xi} est réalisée par le module mélangeur 10 à partir des paramètres applicatifs ai, bi et ci, calculés par le module 12, du poids de pondération perceptuel $\{\varphi i\}$ et de la variance $\{\sigma_{xi}^2\}$ calculés par le module d'analyse du signal 11, et des paramètres d'insertion σ_{wi} et γi estimés par le module 13.

Le module mélangeur comprend un démodulateur 15 qui estime la réponse rx du signal original transformé à une démodulation d'un premier ensemble de porteuses $\{G_j$. Cette démodulation prend en compte les valeurs du poids de pondération perceptuel φi et les valeurs du facteur d'atténuation γi.

Le module mélangeur 10 comprend en outre un générateur de porteuses 16 qui génère le premier ensemble de m porteuses $\{G_j\}$ à partir de clés publiques ou privées. Chaque composante rxj de la réponse du signal original transformé est déterminée à partir de la relation $\sum_{i\in[1,n]}\varphi i\,(\gamma i.xi).G_{ij}$, où G_{ij} désigne le i-ième coefficient de la j-ème porteuse fournie par le générateur de porteuses 16.

Le module mélangeur 10, représenté sur la figure 5, comprend également un module 14 de mise en forme du message propre à fournir m composantes bj définissant le message à insérer, à partir des réponses rxj fournies par le démodulateur 15 et d'un ensemble de mots de code U appliqués au dispositif de mise en forme 14 en même temps que le message de marquage M.

Les valeurs des n coefficients {yi} du signal après marquage sont alors calculées à partir de ces composantes bj, via un modulateur 18, un additionneur 20 et un module de mise à l'échelle 17, selon la relation (6) de l'annexe II de la description.

Plus précisément, pour chacun des bits des clés publiques ou privées, le dispositif générateur de porteuses 16 fournit les porteuses G_{ij} au modulateur 18 pour moduler les composantes bj. Le modulateur 18 effectue une modulation des composantes bj de l'information de marquage par les porteuses G_{ij} pour fournir n coefficients relatifs à l'information de marquage. Le i-ème coefficient relatif à l'information de marquage est donné par la relation $\sum_{j\in[1,m]} bj G_{ij}$.

Le modulateur 18 peut en outre effectuer une modulation en amplitude de ces coefficients relatifs à l'information de marquage, par le terme $k_{2i} = \sigma_{wi} / \sum_{j\in[1,m]} G_{ij}^2$, relatif au terme de pondération de l'énergie du message de marquage σ_{wi} et aux porteuses G_{ij}.

Le modulateur 18 fournit alors au circuit additionneur 20 un nombre n de coefficients relatifs à l'information de marquage de la forme:
$x'i = \sigma_{wi} / \sum_{j\in[1,m]} G_{ij}^2 * \sum_{j\in[1,m]} bj G_{ij}$.

Le circuit additionneur 20 ajoute ces coefficients x'i aux coefficients xi du signal original transformé. Ce résultat est ensuite mis à l'échelle par le module de mise à l'échelle 17 à partir du terme $k_{1i} = \sigma_{xi}^2 / (\sigma_{xi}^2 + \sigma_{wi}^2)$, exprimé en fonction des valeurs de la variance σ_{xi}^2 du signal dans l'espace transformé pour les différents coefficients xi et du terme de pondération σ_{wi} de l'énergie de la marque ajoutée. Ce terme correspond à un filtre de Wiener.

Le module de mise à l'échelle 17 fournit donc le signal marqué de coefficients yi dans l'espace transformé, comme indiqué par la relation (6) de l'annexe II.

Le module de mise en forme 14 du mélangeur 10 est maintenant décrit plus en détail. Le module de mise en forme 14 reçoit un message M à insérer, qui est défini à partir d'un ensemble de mots de code U. Cet ensemble est de taille 2^{C+R} et est découpé en 2^C sous-ensembles U_M. Chacun de ces sous-ensembles comporte 2^R mots de codes et sont associés à chacun des 2^C messages possibles. Les différents mots de codes sont définis dans un espace m-aire et sont tels que :$1/m. \Sigma_j (U^2_{k,j}) = 1$ pour $j \in [1,m]$.

Tout procédé de génération de ces mots de codes et de regroupement de ces mots de codes en sous-ensembles U_M peut être utilisé. Parmi ceux-ci, on peut notamment citer les mots de codes générés par un système de codes correcteurs (par exemple, les C premiers bits sont des bits utiles qui identifient le message, tandis que les R derniers bits sont des bits d'adaptation au signal hôte qui identifient le mot de code utilisé pour le message M).

Le module de mise en forme 14 reçoit en outre la réponse rx du signal original transformé, fournie par le démodulateur 15. Pour déterminer les composantes rxj de cette réponse, le démodulateur 15 en fournit d'abord une estimation selon la relation $\sum_{i\in[1,n]}\varphi i\ (\gamma i.xi).G_{ij}$, indiqué ci-avant. Puis il renormalise cette estimation de façon adéquate en rxj de telle façon que l'insertion des rxj, en utilisant la technique proposée précédemment par la relation (6), compense la réponse du signal hôte au point d'attaque considéré défini par les paramètres d'attaque, que cette attaque soit matérialisée par ajout de bruit et filtrage ou encore par une désynchronisation partielle.

Le module de mise en forme 14 recherche alors un mot de code U_k, parmi les mots de code associés au message M à insérer, en minimisant le critère d'écart quadratique défini par la relation (7) de l'annexe II à la description, à partir de la réponse rx au signal original transformé. Ce mot de code représente un vecteur U_k ayant m composantes U_{kj}.

A partir de ce mot de code U_k et de la réponse rx fournie par le démodulateur 15, le module de mise en forme 14 définit un vecteur V' de dimension m ayant des composantes définies par la relation (8) de l'annexe II, où la notation $<A|B> = \sum AjBj$ représente le produit scalaire entre deux vecteurs A et B.

A partir de ce vecteur V', le module de mise en forme 14 définit un vecteur V de composantes Vj selon la relation (9) de l'annexe II, de telle sorte que le vecteur V soit proportionnel au vecteur V' et que l'on ait $<V|V> = 0$ ou $<V|V> = m$, suivant que V' est nul ou non. En particulier, ce vecteur V a la propriété d'être orthogonal au vecteur U_k.

Le module de mise en forme 14 recherche ensuite la valeur d'un paramètre θ maximisant la relation (10) formulée de l'annexe II, à partir de paramètres u0, v0 et K déterminés en fonction de la réponse au signal original transformé rx, du vecteur U_k et du vecteur V. Ces

paramètres u0, v0 et K sont définis par les relations (11) également incorporées à l'annexe II.

Finalement le module de mise en forme 14 calcule les valeurs des composantes bj à partir du paramètre θ ainsi déterminé, et des composantes U_{kj} et V_j des vecteurs U_k et V, selon la relation (12) de l'annexe II.

Le but du calcul des valeurs des composantes bj est de définir le signal à ajouter de telle sorte que la réponse du démodulateur utilisé lors de l'extraction soit cohérente avec celle du mot de code U_k et la plus robuste possible. La robustesse est définie par l'équation (10). Cette robustesse correspond au niveau d'énergie du bruit pouvant être ajouté sans pour autant sortir du cône associé au mot de code U_k de la figure 6.

En référence à le figure 6, les vecteurs U_k, représenté par le vecteur $\underline{u}$, et le vecteur V, représenté par le vecteur $\underline{v}$, forment une base orthogonale normalisée définissant l'hyperplan contenant le vecteur réponse rx et le vecteur code U_k. Dans cet hyperplan, le déplacement (cos θ, sin θ) définit le signal pouvant être ajouté. La maximisation de l'équation (10) revient alors à rechercher le vecteur de composantes bj maximisant la robustesse. Ramené sur chaque composante de la modulation (i.e. valeurs bj), celui-ci s'exprime alors par l'équation (12).

La figure 6 représente une interprétation géométrique de cette définition. Le cône représenté par la zone hachurée représente l'ensemble des valeurs amenant un décodage correct du mot de code. Sp représente l'ensemble des points qui respectent une contrainte de puissance P du signal pouvant être ajouté (ici P=1) . Le vecteur $\underline{w}$ correspond au vecteur de composantes bj et $\underline{x}$ correspond au vecteur rx. Les hyperboles Hn correspondent aux réponses de robustesse constante (i,e suite à l'ajout d'un bruit d'une énergie donnée).

Un tel principe de définition du signal a été proposé par Cox et al dans un article intitulé "Watermarking as communications with side information", Proc.IEEE, 87(7):1127-1141,1999 dans le cadre d'un tatouage appliqué directement au signal original, et dans un contexte de détection. La détection diffère de l'extraction dans le sens où l'on recherche la présence d'un message U connu. Par ailleurs, l'interprétation du paramètre K de l'équation

(10) diffère. Dans le document de Cox et al le paramètre K est lié à un test d'hypothèse de présence, tandis qu'en extraction, il assure de décoder le bon message (l'ouverture du cône de la figure 6 dépend alors du dictionnaire utilisé - cf équation (11)).

Cette technique visant à limiter l'interférence du signal hôte correspond à la technique de codage canal avec information de bord. Le principe général de cette technique de codage canal a été initialement proposé par Costa dans un article intitulé "Writing on dirty paper", IEEE Trans. Info. Thy, 29(3):439-441, May 1983. Dans le cadre de l'invention cette technique est appliquée sur les informations issues de la démodulation des porteuses G_{ij}.

Le module de définition des paramètres d'insertion globaux 13 définissant les propriétés intrinsèques du dispositif de marquage est décrit plus en détail ci-après. Le module de définition 13 recherche tout d'abord le couple de paramètres globaux (λ,χ), pour définir les paramètres d'insertion.

Le couple (λ,χ) optimal recherché peut être défini en spécifiant deux propriétés parmi les trois suivantes qui sont:
- la distorsion d'insertion D_{xy} entre le signal original x et le signal marqué y, dans l'espace transformé, calculée suivant une relation similaire à celle donnée par la relation(1) de l'annexe II;
- la distorsion d'attaque maximale tolérée $D_{xy'}$ entre le signal original x et le signal marqué resynchronisé y', dans l'espace transformé;
- la mesure de performance Eb/N_0 du système de marquage.

Par exemple, pour des distorsions D_{xy} et $D_{xy'}$ données, le système recherche le couple (λ,χ) conduisant à la plus forte valeur du rapport Eb/N_0, ou pour Eb/N_0 et D_{xy} donnés, le système recherche le couple (λ,χ) conduisant à la plus forte valeur de $D_{xy'}$, ou encore pour Eb/N_0 et $D_{xy'}$ donnés, le système recherche le couple (λ,χ) conduisant à la plus petite valeur de $D_{xy'}$.

Les valeurs de D_{xy}, $D_{xy'}$ et Eb/N_0 sont exprimées en fonction de (λ,χ) selon les relations (13) et (14) formulées dans l'annexe II de la description.

Après avoir déterminé les paramètres globaux d'insertion (λ,χ), le module 13 détermine alors les paramètres d'insertion γi et σ_{wi}. γi et σ_{wi} sont des variables auxiliaires de travail, fonctions

de λ et χ, qui définissent les propriétés d'insertion pour un site i correspondant à la position d'un coefficient xi dans le spectre du signal transformé. Pour un site i, étant donnés les paramètres globaux (λ,χ) et les paramètres locaux ai, bi, ci et σ_{xi}, le couple (γi, σ_{wi}) est déterminé par l'exécution des étapes de l'organigramme représenté sur la figure 8.

A l'étape 100, σ_{wi} est recherché, dans l'intervalle $[0, \varphi i\sqrt{\lambda}\sigma_{xi}^2 / ci]$ qui maximise la fonction (16) de l'annexe II, avec γi donné par la relation (17) de l'annexe II.

A l'étape 102, pour le point trouvé, le dispositif teste si $\gamma i \geq 0$ et $\gamma i \leq [\sigma_{xi}^2 / (\sigma_{xi}^2 + \sigma_{wi}^2)]$:

- Si $\gamma i \geq 0$ et $\gamma i \leq [\sigma_{xi}^2 / (\sigma_{xi}^2 + \sigma_{wi}^2)]$, le couple ($\gamma$i, σ_{wi}) est retenu à l'étape 104;
- Sinon, à l'étape 106, on utilise le couple ($\gamma i=1, \sigma_{wi}=0$). Soit aucun marquage n'est effectué sur ce site.

En particulier, dans le cas où ai = bi :

- si $\lambda > \chi$ ou si $\sigma_{xi} < [ci / (\varphi i\sqrt{ai}\sqrt{(\chi - \lambda)}]$, on utilise le couple ($\gamma$i, σ_{wi}) donné par les relations (18) de l'annexe II;
- sinon, c'est le couple ($\gamma i = 1, \sigma_{wi} = 0$) qui est retenu.

On remarque notamment que lorsque ai = bi = 1, $\sigma_{wi} = \varphi i.\sigma_{xi}^2.\sqrt{\lambda} / ci$.

Une base théorique sur laquelle s'appuient les développements décrits précédemment est la suivante. Les différentes expressions utilisées pour la définition des paramètres d'insertion correspondent aux expressions liées à une modélisation statistique des différents signaux et à un modèle d'attaque assez général. Les coefficients xi sont supposés suivre une loi de probabilité Gaussienne de moyenne 0, et de variance σ_{xi}^2 et être indépendants. Les attaques considérées sont du type "scaling" (facteurs γi) et ajout de bruit gaussien de variance $\sigma_{\delta i}^2$. Soit encore : $yi' = (\gamma i/\gamma_{wi})yi + \delta i$ avec $\gamma_{wi} = \sigma_{xi}^2/(\sigma_{wi}^2 + \sigma_{xi}^2)$.

Le facteur d'échelle permet, en outre, de bien prendre en compte les techniques de filtrage pouvant être appliquées. La nouveauté de l'approche proposée ici est de considérer des signaux non identiquement distribués, l'utilisation d'une métrique perceptuelle, la prise en compte de désynchronisation partielle et l'utilisation d'une technique d'insertion/extraction basée sur l'utilisation d'une modulation type COFDM (acronyme pour "Coded Orthogonal

Frequency Division Multiplex", multiplexage de fréquence orthogonal codé) à étalement de spectre utilisée sur l'ensemble des coefficients.

Afin de définir les paramètres σ_{wi}^2 définissant l'énergie d'insertion, on peut aussi considérer un jeu entre un attaquant et un défenseur selon la théorie des jeux. L'attaquant, connaissant le système utilisé essaie, suivant le principe connu de Kerckoffs, de minimiser la mesure de performance du système Eb/N_0 sous une contrainte de distorsion d'attaque maximale $D_{xy'}\_max$.

Le défenseur cherche quant à lui au contraire à maximiser cette mesure de performance sous une contrainte de distorsion d'insertion maximale D_{xy}_max. Dans le cas présent Eb/N_0 représente le rapport signal à bruit entre l'énergie du message caché et le bruit d'attaque. Ce problème peut alors être résolu en utilisant une formalisation Lagrangienne du problème. On introduit alors les facteurs de Lagrange $\lambda > 0$ et $\chi > 0$, et on considère alors le sous problème suivant dépendant de (λ,χ), à savoir rechercher une solution générale à l'équation (15) définie dans l'annexe II de la description.

La solution générale est définie comme la solution associée au couple (λ,χ) aboutissant à une solution telle que $D_{xy'} = D_{xy'}\_max$ et $D_{xy} = D_{xy}\_max$.

Dans la description ci-dessus, on retrouve la recherche sur (λ,χ) pour respecter les contraintes de distorsion. L'expression à maximiser dans l'étape 100 correspond au terme $\{Eb/N_0 + \lambda.D_{xy'} - \chi.D_{xy}\}$. Les deux derniers termes étant les termes Lagrangiens associés respectivement à la distorsion d'attaque et d'insertion. Les termes liées au contraintes $D_{xy'}\_max$ et D_{xy}_max ont été supprimés, car ils sont constants et également pour des raisons de simplicité.

Il est à noter que la minimisation sur les paramètres d'attaques (γi, $\sigma_{\delta i}$) a déjà été prise en compte notamment dans la définition du paramètre γi dans la première étape.

L'extraction d'un message inséré après attaques se réalise en deux phases dans le dispositif d'extraction 2. Dans un premier temps, une démodulation linéaire est effectuée afin d'obtenir des observations $\hat{bj}$ avec $j \in [1,m]$. Ensuite, le message extrait est défini recherchant le mot de code proche des observations.

Dans le dispositif d'extraction 2, le signal marqué yi est resynchronisé par le module de resynchronisation 8, puis transformé par le module de transformation 7 en une suite de coefficients yi' par une transformation identique à celle qui a été utilisée lors de l'insertion.

Le module d'extraction qui est représenté à la figure 7 comprend un démodulateur 21 couplé à un décodeur du message extrait. Le démodulateur 21 calcule une réponse du signal {yi'} à une démodulation d'un deuxième ensemble de porteuses G_j fournies par un générateur de porteuses 23, selon la relation (19) de l'annexe II. Cette démodulation prend en compte le poids de pondération perceptuel φi calculé à partir d'une analyse effectuée par un module 24 d'analyse du signal yi'.

La démodulation repose sur l'extraction d'une estimation du message inséré $\hat{b}j$ par la relation (19) de l'annexe II, sur l'ensemble des sites marqués.

Il est à noter que tout estimateur définissant une réponse proportionnelle à cet estimateur peut être également considéré.

Dans une variante de réalisation, le deuxième ensemble de porteuses est identique au premier ensemble de porteuses produites par le module générateur de porteuses 16 du module d'insertion.

Le décodage du message a lieu après sa mise en forme estimé $\hat{b}j$. Il consiste à rechercher le mot de code U_k le plus proche des valeurs estimées $\hat{b}j$ par la relation (20) définie dans l'annexe II.

Le message associé au mot de code U_k correspond alors au message extrait. Pour réaliser la recherche du mot de code le plus proche, on peut utiliser un procédé de recherche exhaustive, ou bien encore profiter de toute technique de recherche rapide liée à la définition des mots de codes utilisés, par utilisation de technique de décodage de code canal par exemple.

Il est à noter que l'invention n'est pas limitée aux formes de réalisations décrites ci-dessus.

ANNEXE I

I-1 Signaux :

- n : nombre de coefficients du signal dans le domaine transformé,
- x_i, $i \in [1, n]$: les valeurs des coefficients du signal dans l'espace transformé,
- y_i, $i \in [1, n]$: les valeurs des coefficients du signal dans l'espace transformé après marquage.
- y_i', $i \in [1, n]$: les valeurs des coefficients du signal dans l'espace transformé après marquage, attaques et resynchronisation.
- σ_{xi}^2, $i \in [1, n]$: les valeurs de la variance du signal dans l'espace transformé pour les différents coefficients.
- $D_{xy} = \sum D_{xy}|i$: la distorsion entre deux signaux x et y définie par la relation (1) répertoriée dans l'annexe II à la description.
- φi : poids de pondération perceptuel pour le i_ème coefficient dans la métrique de distorsion. Ces poids sont définis en rapport avec le type de signal traité, la transformation utilisée et les valeurs du signal observée.
- D_{xy}: distorsion d'insertion.
- $D_{xy'}$: distorsion d'attaque.
- (ai, bi, ci): variables identifiant les propriétés du système relatives aux différents coefficients d'insertion (variables comprises entre 0 et 1).
- ai: degré d'interférence avec le signal original.
- bi: degré d'auto interférence du signal inséré.
- ci: paramètre d'atténuation d'un site (par exemple lié à sa sensibilité face aux attaques désynchronisantes); ce terme dépend de l'espace de transformation utilisé et de l'ordre de grandeur de l'erreur de désynchronisation escomptée suite à la resynchronisation effectuée à l'extraction, et des dégradations tolérées.

I-2 Variables de travail :

- (λ,χ) : variables auxiliaires globales de travail permettant de définir les paramètres d'insertion sur chaque coefficient dans le domaine transformé.
- $(\gamma i, \sigma_{wi})$, $i \in \{1, .., n\}$: variables auxiliaires de travail définissant les paramètres d'insertion de chaque coefficient
- γi : facteur d'atténuation
- σ_{wi} terme de pondération de l'énergie de la marque ajoutée.

I-3 Modulation :

- m : nombre de porteuses utilisées lors de l'insertion du message.
- bj avec $j \in \{1, .., m\}$: informations définissant l'information à ajouter pour insérer le message.
- G_{ij} avec $(i, j) \in \{1, .., n\} \times \{1, .., m\}$: informations définissant les porteuses d'insertion du message connues à l'insertion et à l'extraction. Tout procédé de génération de telles porteuses peut être considéré moyennant qu'elles vérifient $E_{i,j} [G_{ij}] = 0$ et $E_{i,j} [G_{ij}^2] = 1$. Elles peuvent être par exemple ainsi générées par l'intermédiaire d'une clé secrète et d'un générateur de nombre aléatoire contrôlé par cette clé secrète.

I-4 Dictionnaire de mots de codes

- 2^C : nombre de messages existants susceptibles d'être insérés dans le signal.
- U : ensemble des mots de codes utilisés. 2^{C+R} mots de codes m aire sont définis, et regroupés en 2^R sous ensembles U_M associés aux différents messages M existants.
- U_k : mot de code utilisé, de taille m et défini par les valeurs $U_{k,j}$ avec $j \in \{1, .., m\}$.

I-5 Paramètre perceptuel

φi : poids perceptuels de distorsion des coefficients du signal.

ANNEXE II

Liste des formules mentionnées dans la description.

$$D_{xy} = \sum_{i \in [1,n]} \varphi i^2 . (xi-yi)^2 \quad (1)$$

$$\sigma_{xi}^2 = (\sum_{j \in vi} xi^2)/|vi| \quad (2)$$

$$\varphi i^2 = 1 / (\sigma_{bi}^2 + Vi^2) \quad (3)$$

$$Vi = (\sum_{j \in vi} |xi|^\rho) / |vi| \quad (4)$$

$$ai = bi = 1 - c^2 i \text{ avec } ci = (\text{sinc}(\Delta i))^d \quad (5),$$

où sinc(x) = sin(πx)/πx et d, la dimension du signal considéré (1 pour un signal audio 1D, 2 pour une image, etc).

$$yi = k_{1i} . (xi + k_{2i} . \sum_{j \in [1,m]} (bj . G_{ij})) \quad (6),$$

avec : $k_{1i} = (\sigma_{xi}^2 / (\sigma_{xi}^2 + \sigma_{wi}^2)$

$k_{2i} = \sigma_{wi} / \sqrt{(\sum_{j \in [1,m]} G_{ij}^2)}$

$$U_k = \arg \min_{Uk \in UM} \{\sum_{j \in [1,m]} (U_{k,j} - rxj)^2\} \quad (7)$$

$$V'j = rxj - \langle rx|U_k\rangle / \sqrt{\langle U_k|U_k\rangle} \quad (8)$$

$$\text{Si } \langle V'|V'\rangle = 0, Vj = 0 \quad (9)$$

Sinon, $Vj = Vj' . \sqrt{m} / \sqrt{\langle V'|V'\rangle}$

$$\{K.(u_0 + \cos\theta)^2 - (v_0 + \sin\theta)^2 \} \quad (10)$$

avec :

$$u_0 = 1/m \langle rx|U_k\rangle \quad (11)$$

~~$v_0 = 1/m \langle rx|V\rangle$~~

$K = 1/ (2^{2.(C+R)/m} - 1)$

$$bj = U_{k,j}.\cos\theta + Vj.\sin\theta \quad (12)$$

$$D_{xy} = \sum_{i=1}^{n} D_{xy}|i$$

$$D_{xy'} = \sum_{i=1}^{n} D_{xy'}|i \quad (13)$$

$$Eb/N_0 = \sum_{i=1}^{n} Eb/N_0|i$$

avec:

$$D_{xy}|i = \varphi i^2(\sigma_{xi}^2\ \sigma_{wi}^2) / (\sigma_{xi}^2+\sigma_{wi}^2) \quad (14)$$

$$D_{xy'}|i = \varphi i^2\ \sigma_{xi}^2\ (1-\gamma i)$$

$$(Eb/N_0)|i = \varphi i^2 \sqrt{\lambda} ci\ \gamma i\ \sigma_{wi}$$

$$\max_{\sigma wi}\ \{\min_{(\gamma i,\ \sigma\delta i)}\{Eb/N_0 + \lambda(D_{xy'} - D_{xy'\_max}) - \chi(D_{xy} - D_{xy\_max})\}\} \quad (15)$$

$$(Eb/N_0)|i + \lambda\ D_{xy'}|i - \chi\ D_{xy}|i \quad (16)$$

$$\gamma i = [\sigma_{xi}^2 - ci\ \sigma_{wi} / (\varphi i\sqrt{\lambda})] / [(1-ai)\sigma_{xi}^2 + (1-bi)\sigma_{wi}^2] \quad (17)$$

$$\sigma_{wi} = [\ A_i.\sigma_{xi}^2 - ci^2 + \sqrt{((A_i.\sigma_{xi}^2 - c^2i)^2 + B_i^{\ 2}.\sigma_{xi}^2)}\ ]\ /\ B_i, \quad (18)$$

$$\gamma i = [\sigma_{xi}^2 - D_i] / [(1-ai)(\ \sigma_{xi}^2 + \sigma_{wi}^2)]$$

avec :

$$A_i = \varphi i^2(\lambda - \chi(1-ai))$$

$$B_i = 2\ \varphi i\ \sqrt{\lambda}\ ci$$

$$D_i = ci.\sigma_{wi}/(\varphi i.\sqrt{\lambda})$$

$$\hat{bj} = \sum_{i\ \epsilon\ Iw} (\varphi i\ yi'\ G_{ij}) \quad (19)$$

avec Iw = ensemble des sites marqués.

$$U_k = \arg\max_{U_k \in U}\{ \sum_{j\in [1,m]}(U_{k,j} - \hat{b}j)^2\} \quad (20)$$

Revendications

1-Dispositif de traitement d'un signal comprenant un module de transformation de signal (5) capable de produire un signal transformé (xi) à partir d'un signal original et un module mélangeur (10) destiné à marquer le signal transformé par un message de marquage (M), caractérisé en ce que le module mélangeur (10) comprend :
- un module de mise en forme (14) capable de calculer une réponse du signal original transformé (rx) à la démodulation d'un premier ensemble de porteuses (Gj) définies par des clés de protection du message et de calculer une information de marquage ({bj}) en fonction de cette réponse et de mots de codes (U) associés au message de marquage,
- un modulateur (18) capable de moduler les informations de marquage fournies par le module de mise en forme (14) par un coefficient donné (Gij) des porteuses du premier ensemble de porteuses, et de moduler en amplitude le coefficient ainsi obtenu par une quantité correspondante liée au terme de pondération de l'énergie du message de marquage et à l'ensemble de porteuses, ce qui fournit un coefficient de marquage,
- un additionneur (20) capable d'ajouter le coefficient de marquage au coefficient correspondant du signal original transformé.

2. Dispositif selon la revendication 1, caractérisé en ce que le module de mise en forme (14) comprend un démodulateur (15) destiné à effectuer la démodulation, ledit démodulateur étant apte à multiplier chaque coefficient du signal original transformé (xi) par le coefficient correspondant d'une porteuse donnée (Gij) du premier ensemble de porteuses, par le poids perceptuel de distorsion (φi) et par le facteur d'atténuation (γi) associés audit coefficient du signal transformé, et à additionner les coefficients ainsi déterminés, ce qui fournit une composante de la réponse du signal original transformé.

3. Dispositif selon l'une des revendications précédentes, caractérisé en ce que le module de mise en forme (14) est apte à calculer l'information de marquage à partir d'un paramètre (θ) prédéterminé, d'un premier vecteur (Uk) associé à un mot de code particulier du message de marquage et d'un deuxième vecteur formant avec ledit premier vecteur une base orthogonale normalisée définissant un hyperplan.

4. Dispositif selon la revendication 3, caractérisé en ce que le mot de code particulier (Uk) est obtenu en minimisant un critère d'erreur quadratique entre les mots de code associés au

message de marquage et la valeur normalisée de la réponse du signal transformé (rx) à la démodulation.

5. Dispositif selon l'une des revendications 3 et 4, caractérisé en ce que chaque composante (Vj) du deuxième vecteur est proportionnelle à la différence entre la composante correspondante de la réponse (rxj)à la démodulation et la projection du vecteur représentant la réponse à la démodulation (rx) sur un vecteur unitaire colinéaire au premier vecteur (Uk/||Uk||).

6.Dispositif selon l'une des revendications 3 à 5, caractérisé en ce que le paramètre (θ) prédéterminé correspond à l'angle entre le vecteur représentant l'information de marquage ({bj}) et le premier vecteur (U_k), ce paramètre (θ) étant déterminé en maximisant la relation:

$$K.(uo + \cos\theta)^2 - (vo + \sin\theta)^2$$

dans laquelle:

- uo représente le produit scalaire entre le vecteur représentant la réponse à la démodulation (rx) et le premier vecteur, divisé par le nombre m de composantes de la réponse à la démodulation,
- vo représente le produit scalaire entre le vecteur représentant la réponse à la démodulation (rx) et le deuxième vecteur (V), divisé par le nombre m,
- $K = 1/(2^{2.(C+R)/m} - 1)$, C et R représentant respectivement le nombre de bits utiles et de bits d'adaptation au signal original et m représente le nombre de composantes de la réponse à la démodulation (rx).

7.Dispositif selon l'une des revendications précédentes, caractérisé en ce que le module mélangeur (10) comprend un module générateur de porteuses (16) propres à générer le premier ensemble des porteuses à partir des clés de protection du message (M).

8. Dispositif selon l'une des revendications précédentes, caractérisé en ce que le mélangeur comporte un module de mise à l'échelle (17) capable de moduler en amplitude chaque coefficient du signal fourni par le circuit additionneur (20) par une quantité liée au terme de pondération de l'énergie du message de marquage (σ_{wi}) et de la variance (σ_{xi}^2) du coefficient correspondant du signal original transformé (xi).

9. Dispositif selon la revendication 8, caractérisé en ce que par ladite quantité est définie par $\sigma_{xi}^2 / (\sigma_{xi}^2 + \sigma_{wi}^2)$, où σ_{xi}^2 est le terme définissant l'énergie du message de marquage et σ_{xi}^2 est la variance du coefficient correspondant du signal original transformé (xi).

10.Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'il comporte un module de transformation inverse (6) en sortie du mélangeur (10), apte à effectuer sur le signal marqué une transformation inverse de celle effectuée par le module de transformation (5).

11.Dispositif selon la revendication 10, caractérisé en ce qu'il comporte un dispositif d'extraction (2) en sortie du module de transformation inverse (6) pour extraire le message du signal marqué, le dispositif d'extraction comportant un module de resynchronisation (8) capable de resynchroniser le signal marqué et un module de transformation de signal (7) apte à transformé le signal marqué resynchronisé, ce qui fournit un signal marqué transformé (yi').

12. Dispositif selon la revendication 11, caractérisé en ce que la transformation réalisée par le module de transformation (7) du dispositif d'extraction est identique à celle réalisée par le module de transformation (5) pour fournir les coefficients du signal original transformés.

13.Dispositif selon l'une des revendications 11 et 12, caractérisé en ce que le dispositif d'extraction (2) est capable de calculer une réponse du signal marqué transformé (yi') à la démodulation d'un deuxième ensemble de porteuses (Gj) définies par des clés de protection du message, ce qui fournit une estimation de l'information de marquage insérée $(\hat{b}j)$.

14.Dispositif selon la revendication 13, caractérisé en ce que le premier ensemble de porteuses et le deuxième ensemble de porteuses sont identiques.

15. Dispositif selon l'une des revendications 11 à 14, caractérisé en ce que le dispositif d'extraction (2) comprend un démodulateur (21) destiné à effectuer la démodulation, ledit démodulateur étant apte à multiplier chaque coefficient du signal marqué resynchronisé (yi') par le coefficient correspondant d'une porteuse donnée (Gij) du deuxième ensemble de porteuses et par le poids perceptuel de distorsion (φi)associé audit coefficient du signal marqué resynchronisé, et à additionner les coefficients ainsi déterminés, ce qui fournit une composante de l'estimation de l'information de marquage $(\hat{b}j)$.

16.Dispositif selon l'une des revendications 11 à 15, caractérisé en ce que le dispositif d'extraction (2) comprend un module générateur de porteuses (16) propres à générer le deuxième ensemble des porteuses à partir des clés de protection du message (M).

17.Dispositif selon l'une des revendications 11 à 16, caractérisé en ce que le dispositif d'extraction (2) comprend un décodeur (22) capable de déterminer le mot de code le plus proche de l'estimation de l'information de marquage ($\hat{bj}$) en maximisant un critère d'erreur quadratique entre un ensemble de mots de code et l'estimation de l'information de marquage, ce qui fournit le message de marquage.

18. Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'il comprend un module de définition de paramètres d'insertion (13) en entrée du module mélangeur (10) capable de déterminer le terme de pondération de l'énergie du message de marquage (σw_i) et le facteur d'atténuation (γi) à partir des propriétés intrinsèques du signal, des contraintes du domaine applicatif, et des propriétés de la transformation utilisée.

19. Dispositif selon la revendication 18, caractérisé en ce que le module de définition de paramètres d'insertion (13) est capable de calculer deux paramètres globaux d'insertion (λ,χ) en fonction de la distorsion d'insertion D_{xy} entre le signal original (x) et le signal marqué (y) dans l'espace transformé, de la distorsion d'attaque maximale tolérée $D_{xy'}$ entre le signal original (x) et le signal marqué resynchronisé (y'), dans l'espace transformé, et du rapport signal à bruit entre l'énergie du message de marquage et le bruit d'attaque Eb/No.

20.Dispositif selon la revendication 19, caractérisé en ce que les deux paramètres globaux d'insertion (λ,χ) sont calculés en recherchant les paramètres λ et χ qui maximise la relation: $Eb/N_0 + \lambda D_{xy'} - \chi D_{xy}$.

21.Dispositif selon la revendication 20, caractérisé en ce que le module de définition de paramètres d'insertion (13) est apte à calculer le terme de pondération de l'énergie du message de marquage (σw_i) et le facteur d'atténuation (γi) à partir des deux paramètres globaux d'insertion (λ,χ) déterminés.

22.Dispositif selon l'une des revendications précédentes, caractérisé en ce que les coefficients du signal original transformé (xi) fournis par le module de transformation du signal (5) sont ceux d'une transformation de Fourier

22.Dispositif selon l'une des revendications 1 à 21, caractérisé en ce que les coefficients du signal original transformé (xi) fournis par le module de transformation du signal (5) sont ceux d'une transformation cosinus.

23.Dispositif selon l'une des revendications 1 à 21, caractérisé en ce que les coefficients du signal original transformé (xi) fournis par le module de transformation du signal (5) sont ceux d'une transformation en ondelettes.

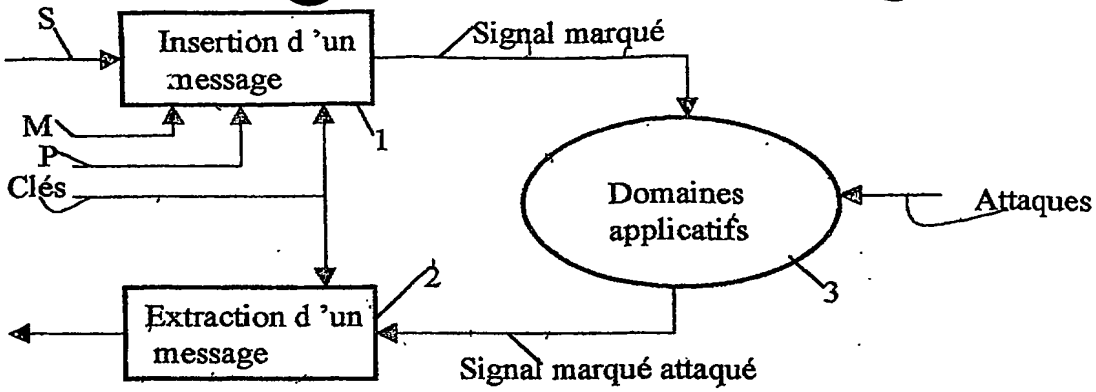


FIG: 1

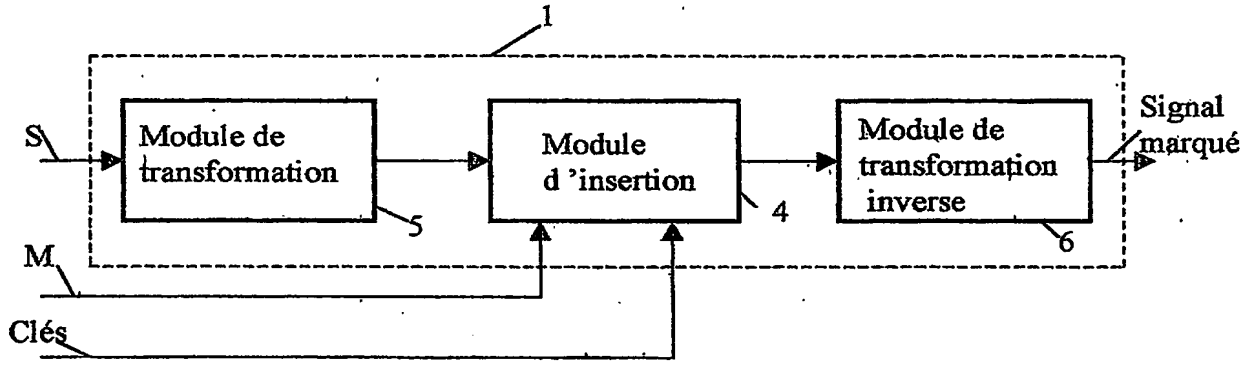


FIG:2

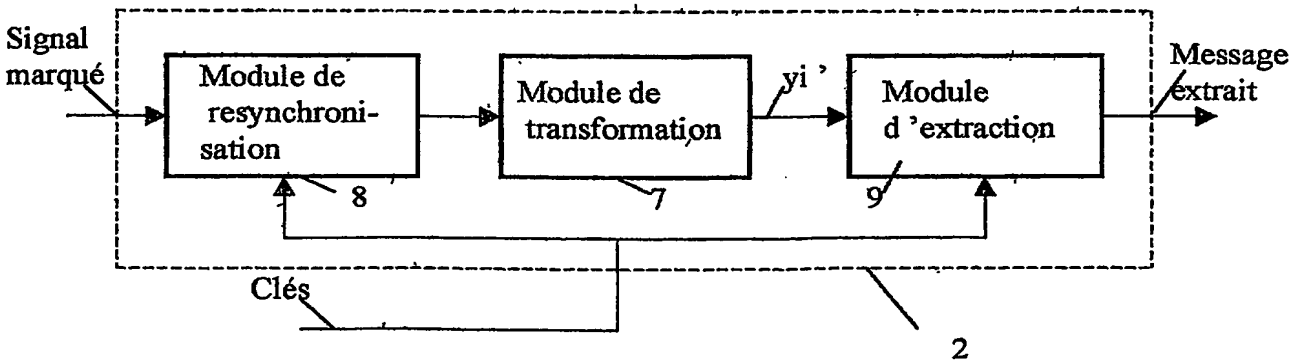


FIG: 3

CABINET NETTER

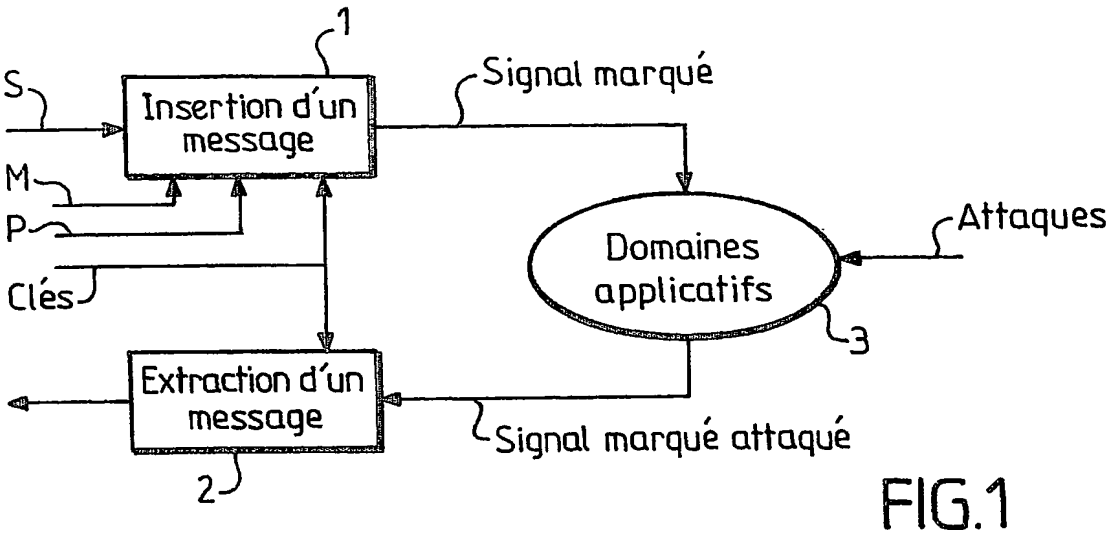


FIG.1

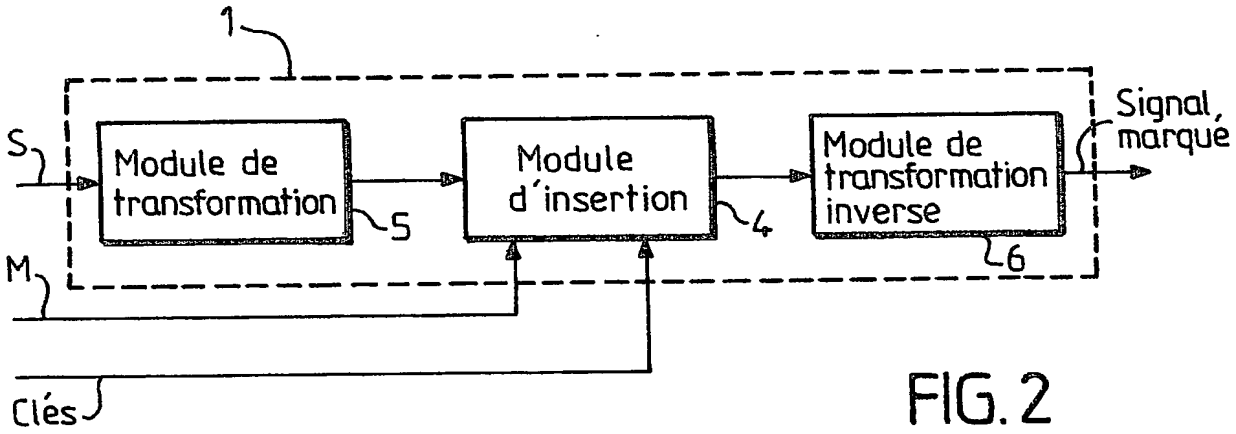


FIG.2

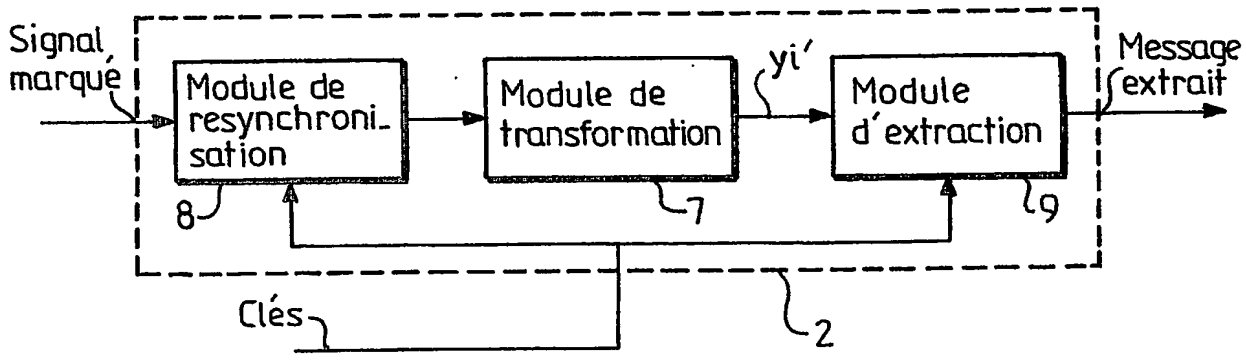


FIG.3

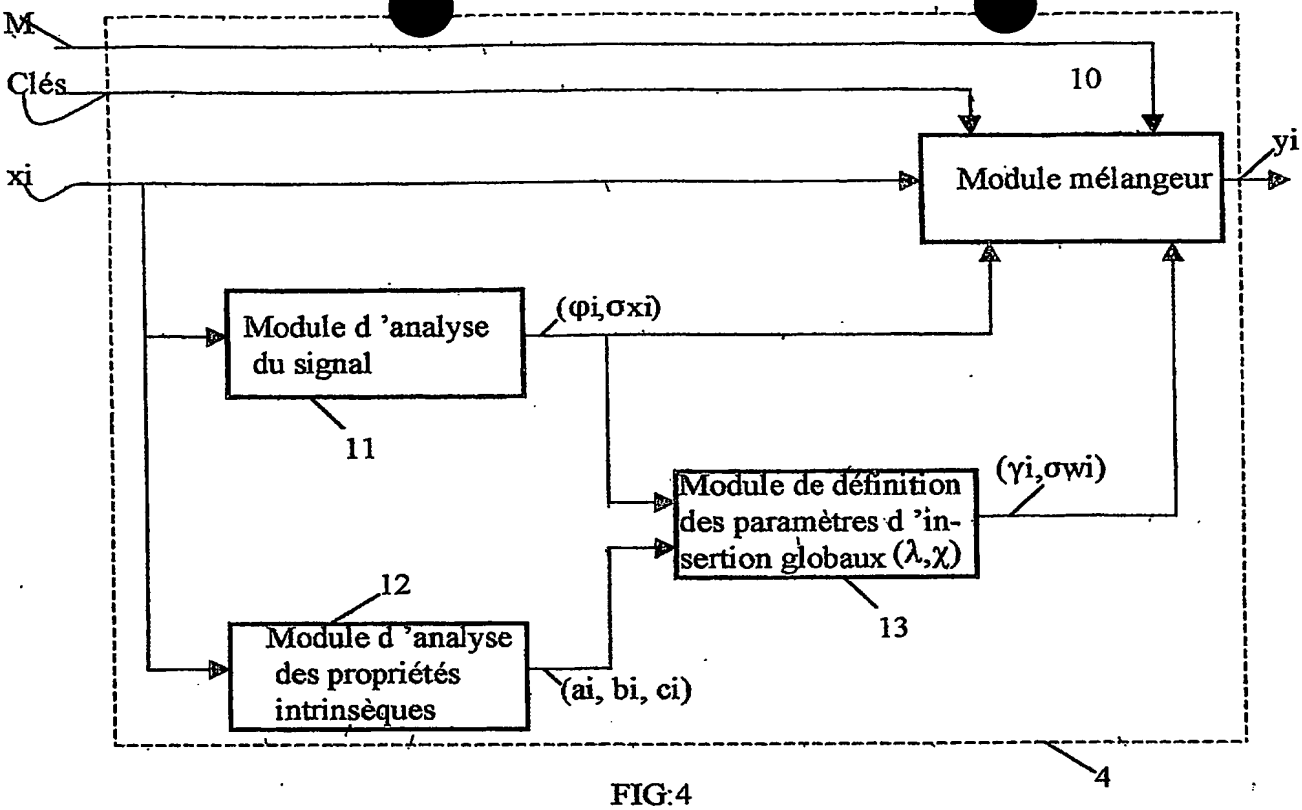


FIG:4

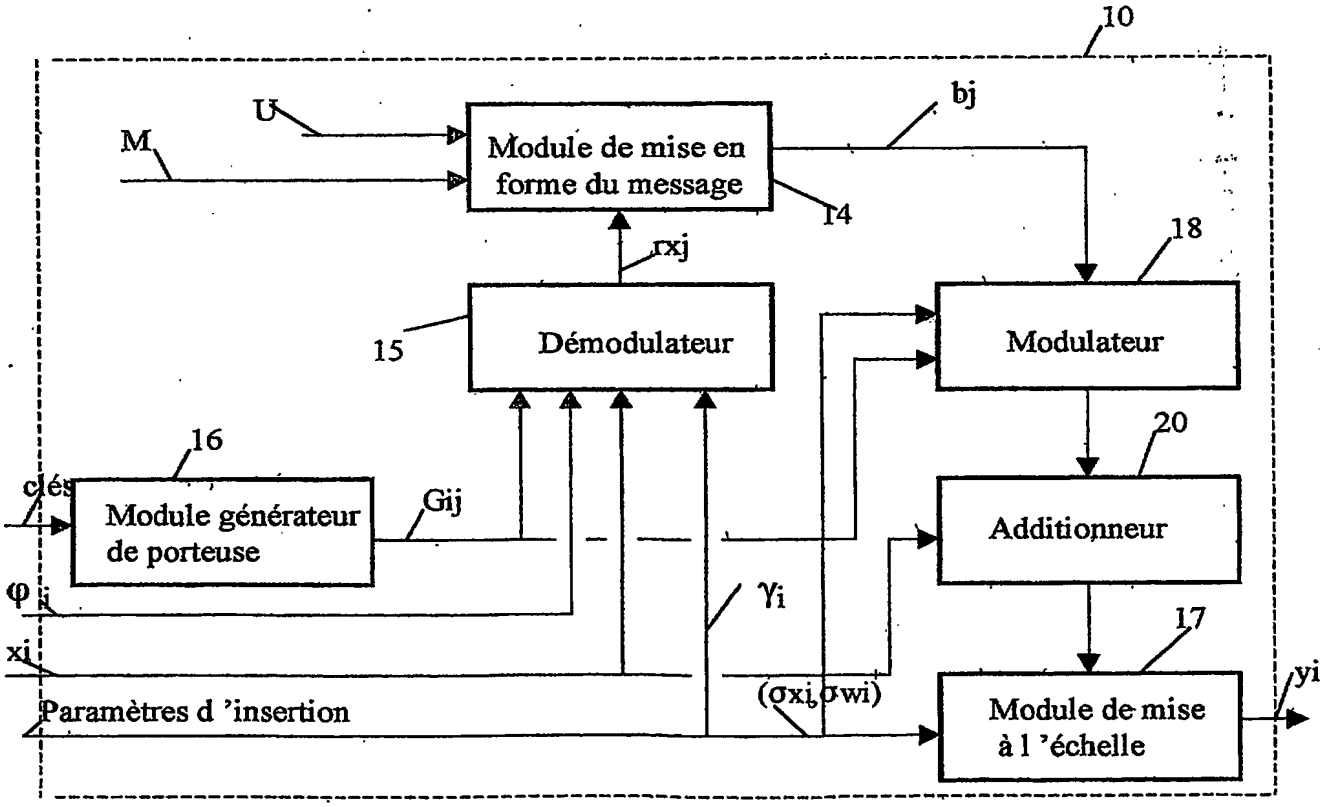


FIG:5

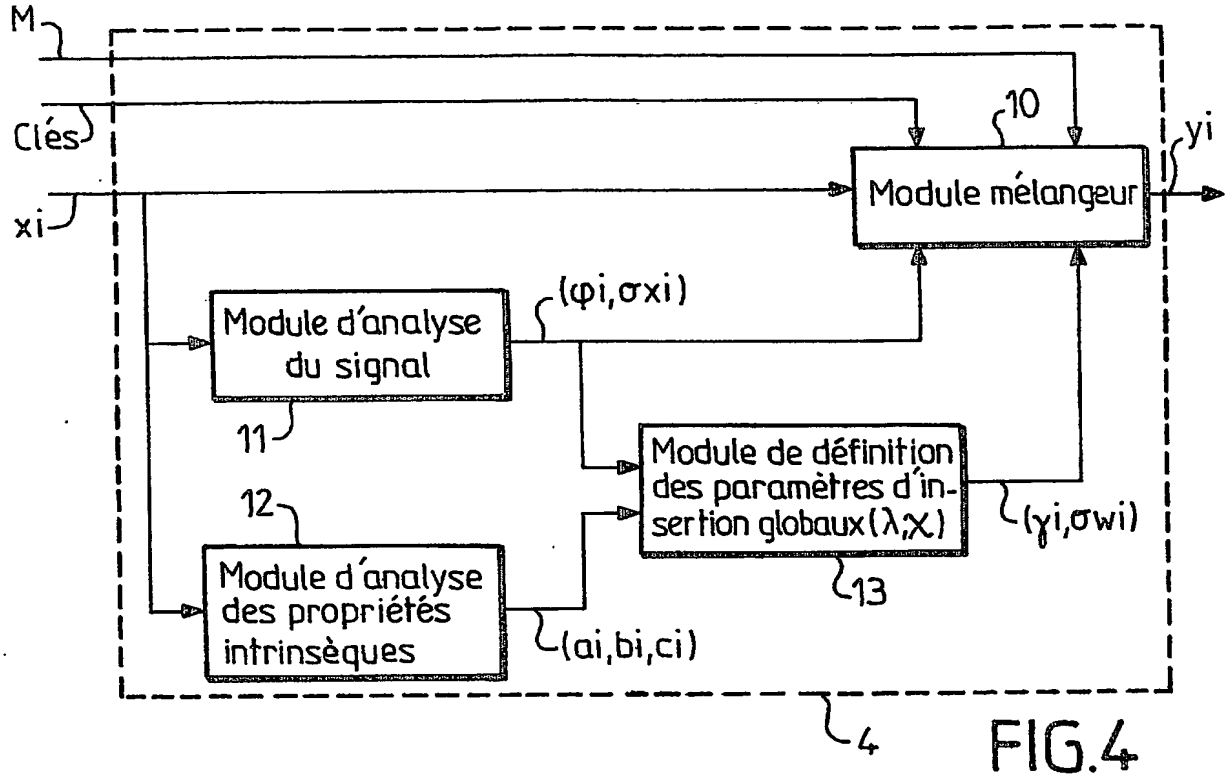

M
Clés
xi
10
yi
Module mélangeur
Module d'analyse du signal
(φi,σxi)
11
Module de définition des paramètres d'insertion globaux (λ;χ)
(γi,σwi)
13
12
Module d'analyse des propriétés intrinsèques
(ai,bi,ci)
4

FIG.4

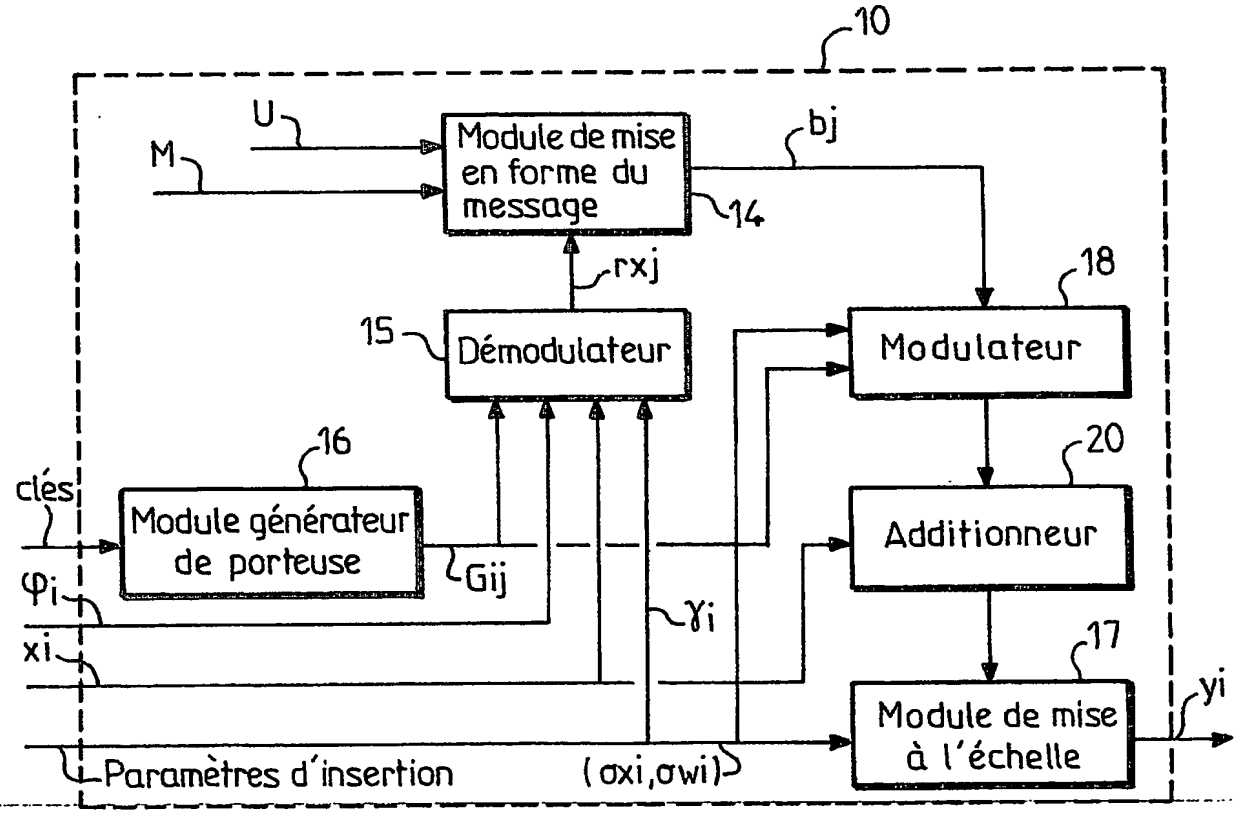

10
U
M
Module de mise en forme du message
bj
14
rxj
18
15
Démodulateur
Modulateur
16
20
clés
Module générateur de porteuse
Gij
Additionneur
φi
γi
xi
17
yi
Module de mise à l'échelle
Paramètres d'insertion
(σxi,σwi)

FIG.5

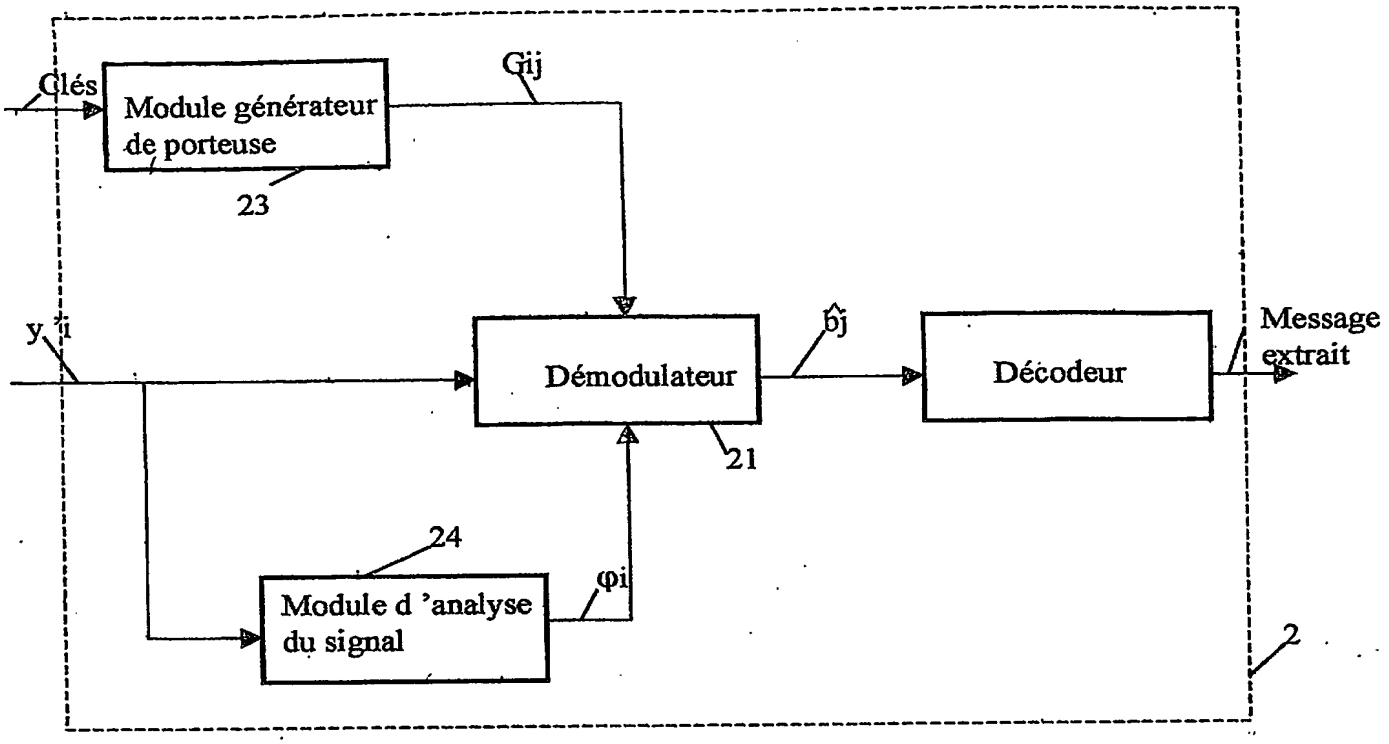


FIG: 7

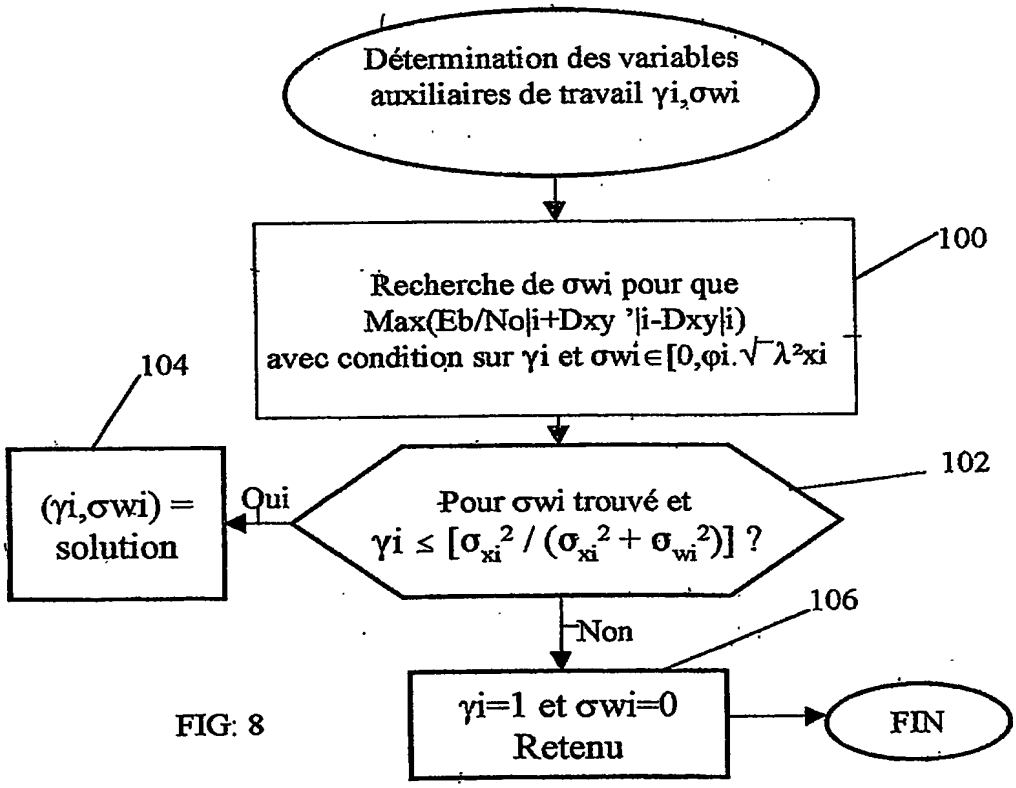


FIG: 8

CABINET NETTER

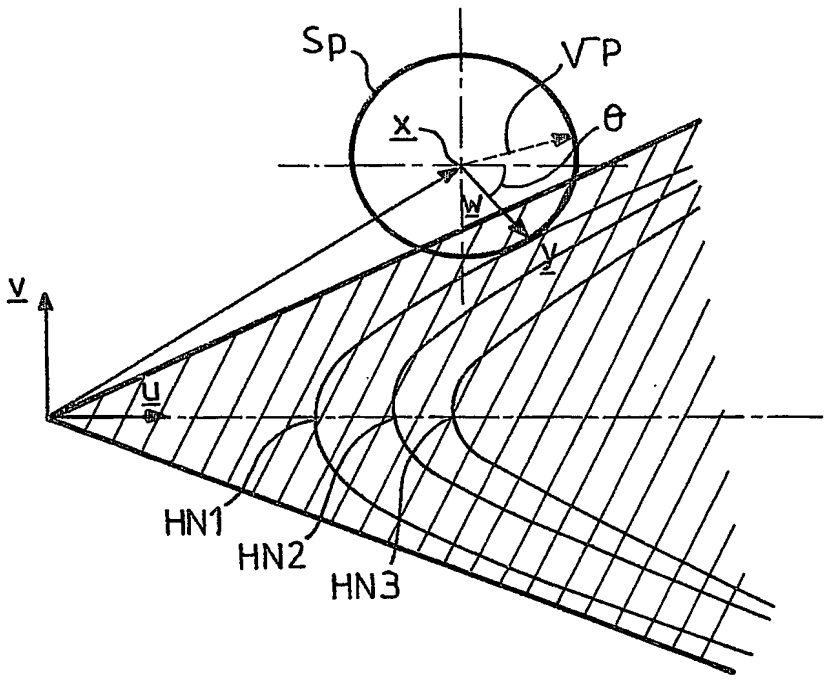


FIG.6

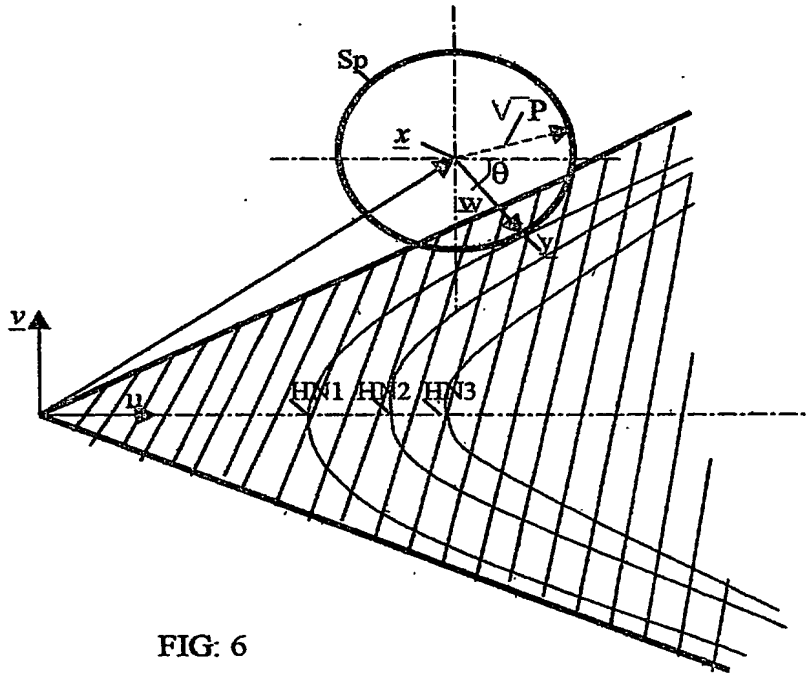


FIG: 6

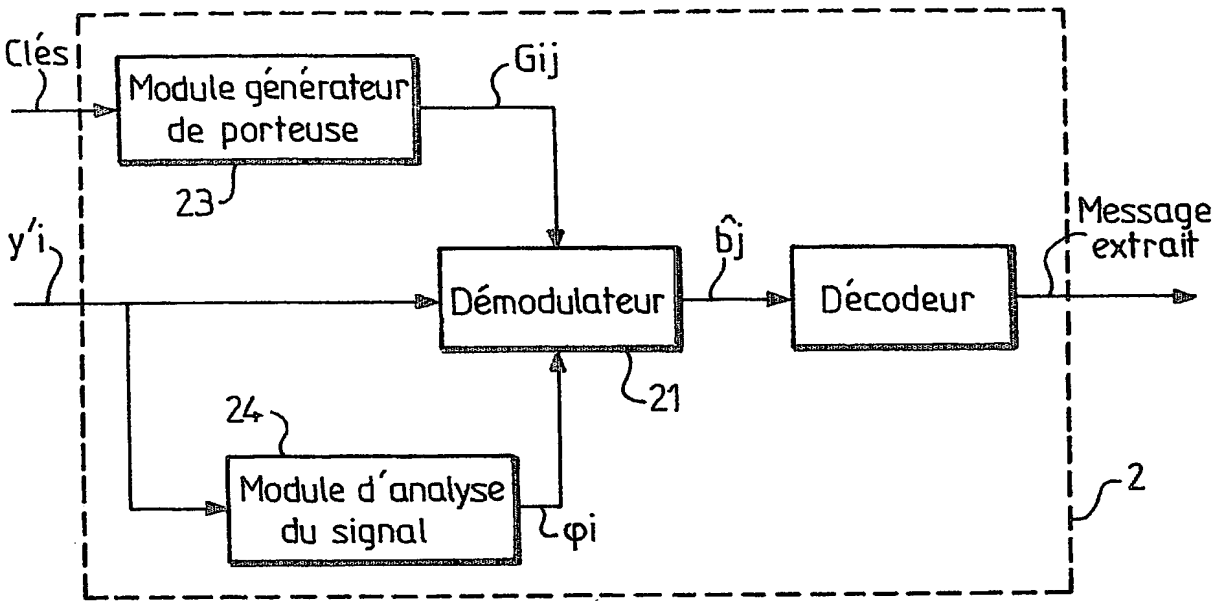

Clés
Module générateur de porteuse
Gij
23
y'i
Démodulateur
b̂j
Décodeur
Message extrait
21
24
Module d'analyse du signal
φi
2

FIG.7

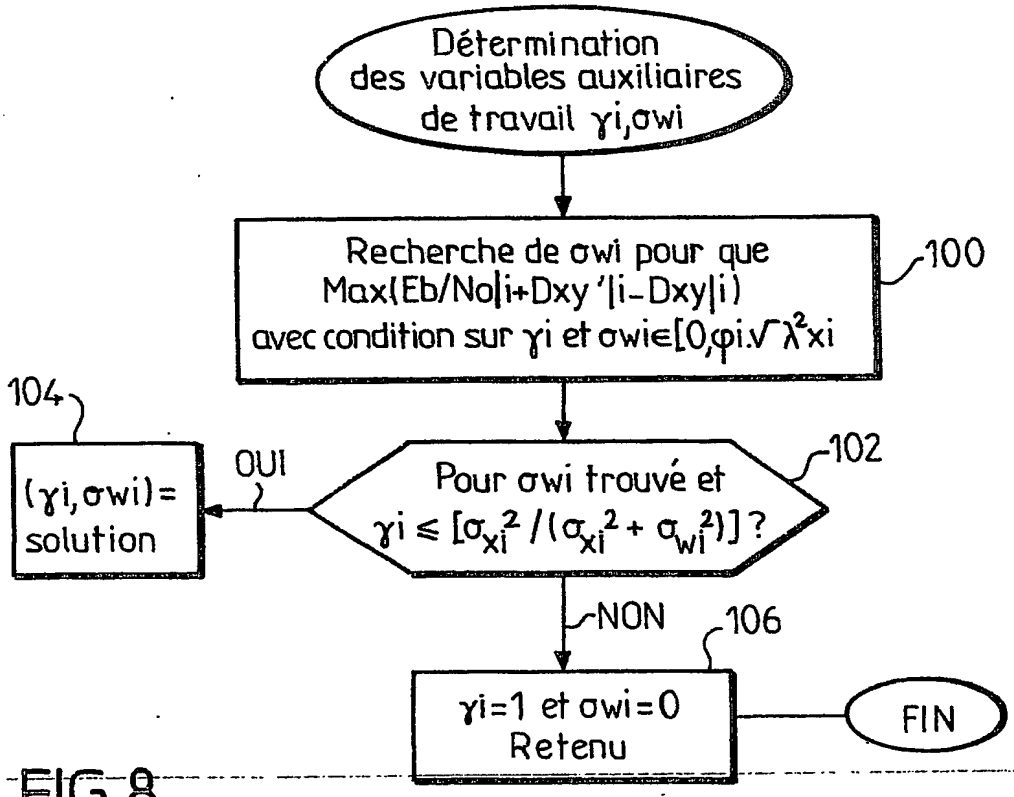

Détermination des variables auxiliaires de travail γi,σwi
Recherche de σwi pour que Max(Eb/No|i+Dxy'|i-Dxy|i) avec condition sur γi et σwi∈[0,φi.√λ²xi
100
104
(γi,σwi)= solution
OUI
Pour σwi trouvé et γi ≤ [σxi² /(σxi² + σwi²)] ?
102
NON
106
γi=1 et σwi=0 Retenu
FIN

FIG.8

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	INRIA CAS 58 (120818)
N° D'ENREGISTREMENT NATIONAL	02 13605

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Dispositif pour le marquage et la restitution de signaux multimedia

LE(S) DEMANDEUR(S) :

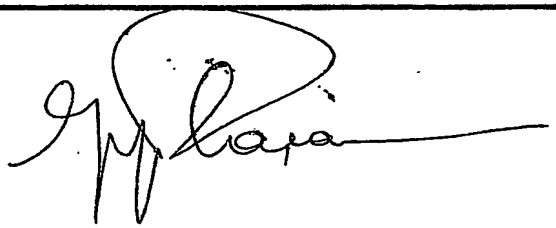
INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		GUILLEMOT	
Prénoms		Christine	
Adresse	Rue	2 allée Françoise Dolto	
	Code postal et ville	35135	CHANTEPIE
Société d'appartenance *(facultatif)*			
Nom		PATEUX	
Prénoms		Stéphane	
Adresse	Rue	9 rue du Général de Gaulle	
	Code postal et ville	35760	SAINT GREGOIRE
Société d'appartenance *(facultatif)*			
Nom		LE GUELVOUIT	
Prénoms		Gaétan	
Adresse	Rue	94 rue Paul Féval	
	Code postal et ville	35000	RENNES
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)

Paris, le 23 juin 2003
Jean-Yves PLAÇAIS
92.1197 (B) (M)



This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.